# OPC UA Configuration Manager

# Inhaltsverzeichnis

**OPC UA Configuration Manager** ..... 1
**Inhaltsverzeichnis** ..... 2
OPC UA Configuration Manager ..... 4
Übersicht ..... 4
**OPC UA Configuration Manager** ..... 5
Serverendpunkte ..... 5
Vertrauenswürdige Clients ..... 7
Ermittlungsserver ..... 7
Vertrauenswürdige Server ..... 8
Instanzzertifikate ..... 10
**Verbindungsbeispiele** ..... 13
**Tipps zur Problembehandlung** ..... 15
Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen ..... 15
Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird ..... 15
Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden ..... 16
Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort) ..... 16
Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden ..... 16
Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll ..... 16
**Ereignisprotokollmeldungen** ..... 18
Konto '<Name>' hat keine Berechtigung zum Ausführen der Anwendung. ..... 18
Das Zertifikat des UA Server wurde erneut ausgestellt. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. ..... 18
Das Zertifikat des UA Client Treibers wurde erneut ausgestellt. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. ..... 18
Das UA Client Zertifikat '<Client-Name>' wurde zurückgewiesen. Der Server kann keine Verbindungen von dem Client annehmen. ..... 18
Das UA Client Zertifikat '<Client-Name>' wurde als vertrauenswürdig eingestuft. Der Server kann Verbindungen von dem Client annehmen. ..... 18
Das UA Server Zertifikat '<Servername>' wurde zurückgewiesen. Der UA Client Treiber kann keine Verbindung zum Server herstellen. ..... 19
Das UA Server Zertifikat '<Servername>' wurde als vertrauenswürdig eingestuft. Der UA Client Treiber kann eine Verbindung zum Server herstellen. ..... 19
Das UA Server Zertifikat '<Servername>' wurde zur Liste der vertrauenswürdigen Server hinzugefügt. Der UA Client Treiber kann jetzt eine Verbindung zum Server herstellen. ..... 19
Das UA Client Zertifikat '<Client-Name>' wurde zur Liste der vertrauenswürdigen Clients hinzugefügt. Der UA Server kann jetzt Verbindungen vom Client annehmen. ..... 19
Das UA Client Zertifikat '<Client-Name>' wurde aus der Liste der vertrauenswürdigen Clients entfernt. Der UA Server kann keine Verbindungen vom Client annehmen. ..... 19
Das UA Server Zertifikat '<Servername>' wurde aus der Liste der vertrauenswürdigen Server entfernt. Der UA Client Treiber kann keine Verbindung zum Server herstellen. ..... 19
Der Endpunkt '<URL>' wurde zum UA Server hinzugefügt. ..... 19

Der Endpunkt '<URL>' wurde vom UA Server entfernt. ..... 19
Der UA Discovery Server '<Servername>' wurde hinzugefügt. Die UA Server Endpunkte können jetzt mit diesem UA Discovery Server registriert werden. ..... 19
Der UA Discovery Server '<Servername>' wurde entfernt. Die UA Server Endpunkte können nicht länger mit diesem UA Discovery Server registriert werden. ..... 20
Der Endpunkt '<URL>' wurde deaktiviert. ..... 20
Das Zertifikat des UA Client Treibers wurde importiert. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. ..... 20
Das Zertifikat des UA Server wurde importiert. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. ..... 20
Der Endpunkt '<URL>' wurde aktiviert. ..... 20
Vertrauenswürdigen Client hinzufügen ..... 20
Vertrauenswürdigen Client entfernen ..... 20
Vertrauenswürdigen Client ablehnen ..... 20
Vertrauenswürdigem Client vertrauen ..... 20
Vertrauenswürdigen Server hinzufügen ..... 20
Vertrauenswürdigen Server entfernen ..... 20
Vertrauenswürdigen Server ablehnen ..... 21
Vertrauenswürdigem Server vertrauen ..... 21
Endpunkt hinzufügen ..... 21
Endpunkt aktivieren ..... 21
Endpunkt deaktivieren ..... 21
Endpunkt entfernen ..... 21
Ermittlungsserver hinzufügen ..... 21
Ermittlungsserver entfernen ..... 21
Client-Zertifikat erneut ausstellen ..... 21
Serverzertifikat erneut ausstellen ..... 21
**Index** ..... **22**

# OPC UA Configuration Manager

Hilfe-Version 1.042

## INHALT

**Übersicht**
Was ist OPC Unified Architecture und wie wird sie verwendet?

**OPC UA Configuration Manager**
Wo finde ich Informationen zu den Registerkarten in OPC UA Configuration Manager ?

**OPC UA Lernprogramm**
Wo finde ich ein Lernprogramm zur Implementierung von OPC UA?

**Verbindungsbeispiele**
Wo finde ich Beispiele für Verbindungen und Informationen zu optimalen Vorgehensweisen im Zusammenhang mit OPC UA?

**Tipps zur Problembehandlung**
Wo finde ich Beschreibungen zu häufigen Problemen?

**Ereignisprotokollmeldungen**
Welche Meldungen enthält das Ereignisprotokoll?

## Übersicht

OPC Unified Architecture (UA) ist ein offener Standard, der durch die OPC Foundation mit Unterstützung Dutzender von Mitgliedsorganisationen erstellt wurde. Obgleich UA beabsichtigt, einen plattformunabhängigen Interoperabilitätsstandard bereitzustellen (weg von Microsoft COM) stellt UA keinen Ersatz für OPC Data Access (DA) Technologien dar. Für die meisten Industrieanwendungen ergänzt oder erweitert UA eine bestehende DA-Architektur. Es handelt sich nicht um einen systemweiten Ersatz. OPC UA ergänzt OPC DA Infrastrukturen auf folgende Weise:

- UA bietet auch eine sichere Methode für die Konnektivität zwischen Client und Server, ohne von Microsoft DCOM abhängig zu sein, und ermöglicht, durch Firewalls und über VPN-Verbindungen eine sichere Verbindung herzustellen. Für Benutzer, die innerhalb eines Unternehmensnetzwerks (innerhalb der Firewall) auf einer Domäne eine Verbindung zu einem Remote-Computer herstellen, sind OPC DA und eine DCOM-Verbindung möglicherweise ausreichend.
- Sie stellt eine zusätzliche Möglichkeit bereit, Fabrikdaten gemeinsam für Geschäftssysteme zu nutzen (von der Fabrik bis zur obersten Ebene). OPC UA kann Daten aus mehreren OPC DA-Quellen in Nicht-Industriesystemen aggregieren.

Für die Mehrzahl von Benutzeranwendungen sind dies die relevantesten Komponenten des UA-Standards:

- Sichere Verbindungen über vertrauenswürdige Zertifikate für Client- und Serverendpunkte
- Robustes Element-Abonnement-Modell, für das Bereitstellen effizienter Datenaktualisierungen zwischen Clients und Servern
- Eine verbesserte Methode zum Ermitteln verfügbarer Informationen von beteiligten UA-Servern

# OPC UA Configuration Manager

Der OPC UA Configuration Manager hilft Benutzern bei der Verwaltung der Konfigurationseinstellungen für den UA Server. Die Sicherheit für OPC UA erfordert, dass alle an der UA-Kommunikation beteiligten Endpunkte über eine sichere Verbindung kommunizieren. Um diese Sicherheitsanforderung zu erfüllen, muss jede UA Server-Instanz und jede UA Client-Instanz ein vertrauenswürdiges Zertifikat bereitstellen, um sich zu identifizieren. Diese Zertifikate können selbstsigniert sein. Als solche müssen sie dem lokalen vertrauenswürdigen Zertifikatspeicher sowohl auf den Server- als auch auf den Client-Knoten durch einen Benutzer mit Administratorberechtigungen hinzugefügt werden, bevor versucht werden kann, sichere UA Client-/Server-Verbindungen herzustellen. Der OPC UA Configuration Manager ist eine benutzerfreundliche Benutzeroberfläche, über die der Zertifikataustausch durchgeführt werden kann.

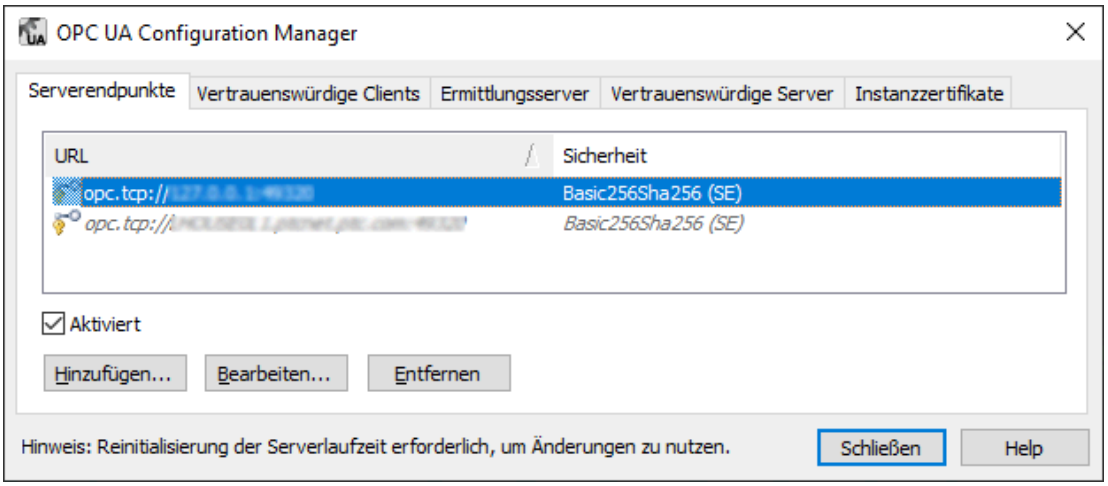
*Weitere Informationen zu einer spezifischen OPC UA Configuration Manager Eigenschaft finden Sie unter den nachfolgenden Links.*

Serverendpunkte
Vertrauenswürdige Clients
Ermittlungsserver
Vertrauenswürdige Server
Instanzzertifikate

## Serverendpunkte

Der OPC UA Server erfordert Serverendpunkt-Definitionen, um eine UA Benutzeroberfläche zu erstellen, mit der UA-Clients kommunizieren können. UA-Server-Endpunkte sind als URLs (Universal Resource Locators) definiert und identifizieren die bestimmte Instanz eines Servers, Transporttyps, sowie die Sicherheit, mit der kommuniziert wird. Ein Serverendpunkt besteht aus einer URL und einem Sicherheitsrichtlinien-Typ. Es sind maximal 100 Serverendpunkte in einem Projekt erlaubt. Die Registerkarte "Serverendpunkte" zeigt u.U. mehrere Serverendpunkte in einer Zeile an.

**Hinweis**: Jeder neu definierte Endpunkt ist standardmäßig aktiviert, kann jedoch, falls gewünscht, vom Benutzer deaktiviert werden. Werden Endpunkte hinzugefügt, entfernt oder geändert, während der Server ausgeführt wird, so muss die Laufzeit des UA Servers neu initialisiert werden.

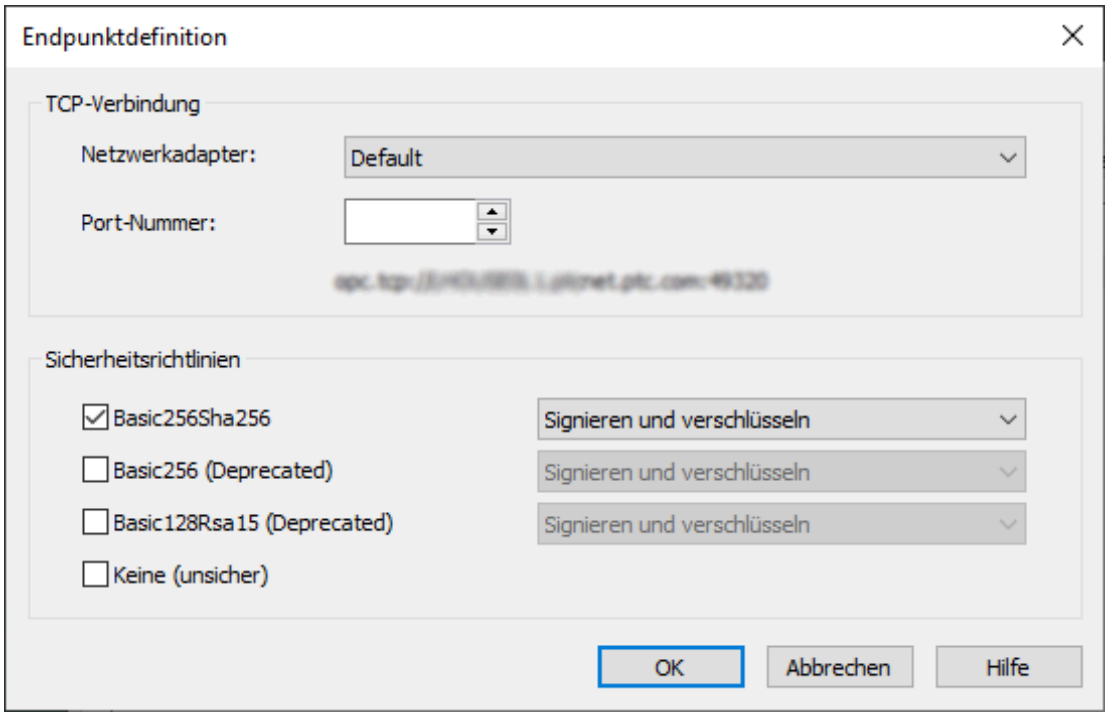



**Hinweis**: Alle Endpunkte innerhalb der Serverinstanz teilen dasselbe Instanzzertifikat. Der UA Server verwendet standardmäßig selbstsignierte Zertifikate, Benutzer können jedoch auf der Registerkarte Instanzzertifikate eine benutzerdefinierte Instanz importieren.

**Wichtig**: Gemäß den OPC UA Anforderungen, muss ein Server, welcher das standardmäßige UA Server-Profil implementiert, das Anmelden mit Benutzername und Passwort unterstützen. Dieser UA Server unterstützt die Validierung von Benutzerinformationen pro Serverinstanz (anstatt von pro Endpunkt). Erkannte Benutzer stammen aus der Funktion "Benutzermanager" innerhalb der Serververwaltung, die sich in der Taskleiste befindet.

### Endpunktdefinition

Klicken Sie auf der Registerkarte "Serverendpunkte" auf **Hinzufügen...** oder **Bearbeiten...** um das Dialogfenster "Endpunktdefinition" zu öffnen.




**Netzwerkadapter**: Dieser Parameter gibt den Netzwerkadapter, an den die Verbindung gebunden wird, an. Er kann für verfügbare Adapter mit IP-Adressen, Standard oder lediglich lokalen Host konfiguriert werden. Die anfängliche Auswahl ist Standard, d.h. es wird eine Zuordnung zu einem Standard-Netzwerkadapter hergestellt.

**Port-Nummer**: Dieser Parameter gibt die Port-Nummer an. Dieser Parameter ist für die Definition erforderlich, da der restliche Teil der URL, welche für die Definition des Endpunkts konstruiert ist, auf dem Hostnamen des Computers und dem Transportprotokoll standardisiert ist. Alle von diesem Dialogfenster definierten Endpunkt-URLs haben das folgende Format: *opc.tcp://<Hostname>:<Port>*. Für den Fall, dass kein vollständig qualifizierter Hostname bestimmt werden kann, wird entweder der lokale Host oder eine IP-Adresse verwendet.

**Sicherheitsrichtlinien**: Diese Sicherheitsrichtlinien- und Meldungsmodus-Parameter geben die vom UA Server unterstützten Sicherheitsalgorithmen an. Basic256Sha256 ist standardmäßig ausgewählt. Die folgenden Optionen sind möglich:

- Basic256Sha256
- Basic256 (Deprecated)
- Basic128Rsa15 (Deprecated)
- Keine (unsicher)

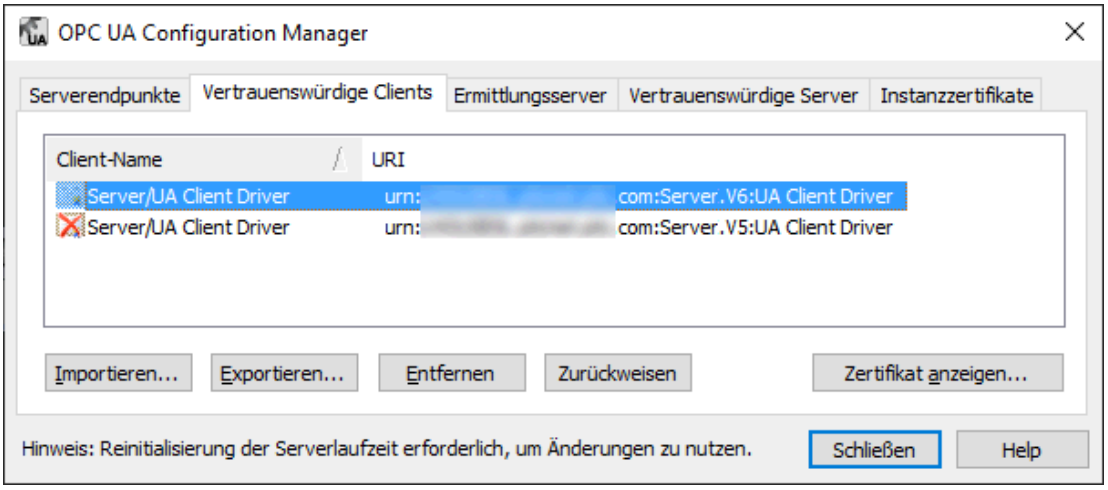
Auf das Dropdown-Menü für die Sicherheitsrichtlinie kann nur dann zugegriffen werden, wenn das entsprechende Kontrollkästchen aktiviert ist. Ist keine der Sicherheitsrichtlinien aktiviert, so wird angenommen, dass die Standard-Sicherheitsrichtlinie "Keine" ist. Diese Auswahl wird nicht empfohlen, da sie keine Sicherheit bietet. Jedes Dropdown-Menü listet die Verschlüsselungsmodi, die vom UA Server unterstützt werden, auf. Sortiert sind die Modi in absteigender Reihenfolge, d.h. von am sichersten bis am wenigsten sicher. Die Standardauswahl ist "Signieren und verschlüsseln". Die folgenden Optionen sind möglich:

- Signieren und verschlüsseln
- Signieren; Signieren und verschlüsseln
- Signieren

**ACHTUNG**: Die Sicherheitsrichtlinien Basic128Rsa15 und Basic256 werden von der OPC Foundation ab der OPC UA-Spezifikation Version 1.04 als veraltet angesehen. Die von diesen Richtlinien bereitgestellte Verschlüsselung ist weniger sicher und die Verwendung der Richtlinien sollte auf das Bereitstellen von Abwärtskompatibilität beschränkt werden.

## Vertrauenswürdige Clients

UA Server benötigen ein Zertifikat, um eine vertrauenswürdige Verbindung zu jedem UA-Client herzustellen. Damit der Server Verbindungen von einem Client mit selbstsigniertem Zertifikat akzeptiert, muss das Zertifikat des Clients in den Zertifikatspeicher des vertrauenswürdigen Client, der von der OPC UA Server Benutzeroberfläche verwendet wird, importiert werden. Um dies zu ermöglichen, kann der UA Configuration Manager vertrauenswürdige Client-Zertifikate importieren, entfernen und anzeigen.




**Importieren...**: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Client-Zertifikat importiert.

**Exportieren...**: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Client-Zertifikat an einen gewünschten Speicherort exportiert.

**Entfernen**: Wird diese Schaltfläche geklickt, so wird das Vertrauen aus dem Client-Zertifikat entfernt. Außerdem wird das Zertifikat aus der Liste der vertrauenswürdigen Clients entfernt.

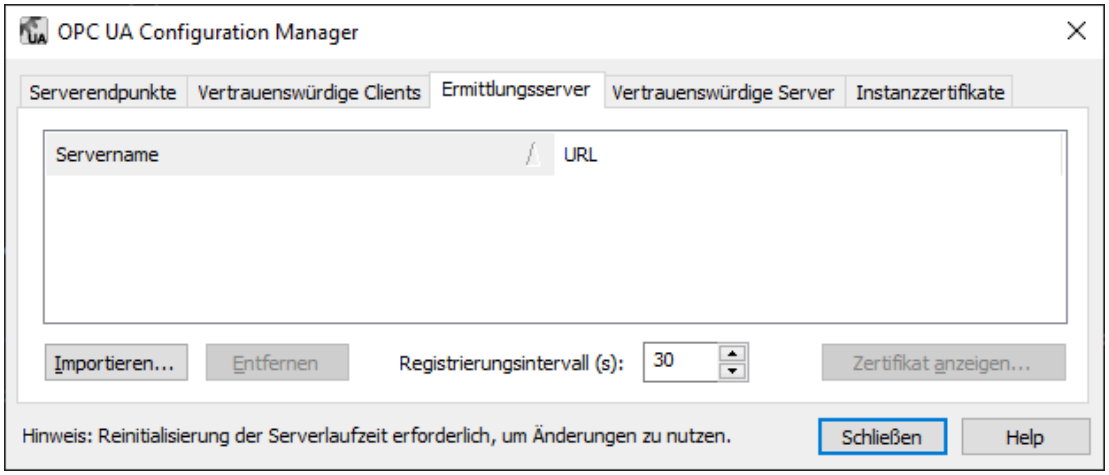
**Zurückweisen**: Wird diese dynamische Schaltfläche geklickt, so wird Vertrauen aus einem Client-Zertifikat entfernt. Zurückgewiesene Zertifikate verbleiben in der Liste der vertrauenswürdigen Clients und werden mit einem roten X gekennzeichnet.

**Vertrauen**: Wird diese dynamische Schaltfläche geklickt, so wird einem Client-Zertifikat vertraut.

**Zertifikat anzeigen...**: Wird diese Schaltfläche geklickt, so werden Informationen zum Client-Zertifikat angezeigt.

## Ermittlungsserver

Jeder OPC UA-Server kann sich mit einem UA-Ermittlungsserver registrieren, damit Clients mit den entsprechenden Berechtigungen auf seine Endpunkt-Informationen zugreifen können. Für das Durchführen dieser Registrierung muss die UA-Server-Benutzeroberfläche wissen, welcher Endpunkt bzw. welche Endpunkte verwendet werden sollen. Ein Ermittlungsserver mit einem selbstsignierten Zertifikat muss abgerufen und im vertrauenswürdigen Zertifikatspeicher des UA-Servers gespeichert werden. Desgleichen muss das Zertifikat des UA-Servers abgerufen werden und im vertrauenswürdigen Zertifikatspeicher des UA-Ermittlungsservers gespeichert werden. OPC UA Configuration Manager ermöglicht das Importieren, Entfernen und Anzeigen vertrauenswürdiger Ermittlungsserver-Endpunkte, die für die UA-Server-Benutzeroberfläche identifiziert werden.

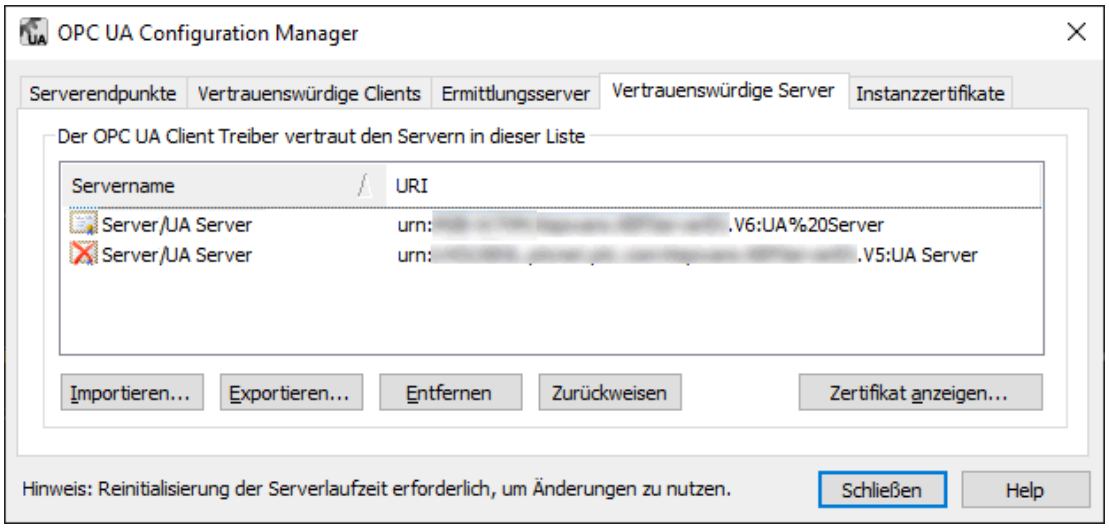



**Hinweis**: Benutzer können das Registrierungsintervall, welches zum Aktualisieren des Ermittlungsservers verwendet wird, über den Parameter **Registrierungsintervall** ändern. Die Standardeinstellung ist 30 Sekunden.

## Vertrauenswürdige Server

Die Registerkarte "Vertrauenswürdige Server" wird nur angezeigt, wenn der UA Client-Treiber auf dem Computer installiert ist. Das Dialogfenster wird verwendet, um eine Liste von vertrauenswürdigen Servern, mit denen der UA Client-Treiber kommunizieren kann, zu erstellen.

**Hinweis**: Der UA Client-Treiber erfordert eine vertrauenswürdige Zertifikatsverwaltung für Clients, die selbst signieren, genau wie der UA Server. Damit der UA Client-Treiber eine Verbindung zu einem Server, der ein selbstsigniertes Zertifikat verwendet, herstellen kann, müssen Benutzer mit Administratorberechtigungen das Zertifikat des externen UA Servers in den vertrauenswürdigen Zertifikatspeicher des UA Client-Treibers importieren. Da der Client-Treiber sein Zertifikat selbst signiert, muss dieses Zertifikat exportiert und im vertrauenswürdigen Zertifikatspeicher des Servers gespeichert werden.




**Importieren...**: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Serverzertifikat importiert.

**Exportieren...**: Wird diese Schaltfläche geklickt, so wird ein vertrauenswürdiges Serverzertifikat an einen gewünschten Speicherort exportiert.

**Entfernen**: Wird diese Schaltfläche geklickt, so wird das Vertrauen aus dem Serverzertifikat entfernt. Außerdem wird das Zertifikat aus der Liste der vertrauenswürdigen Server entfernt.

**Zurückweisen**: Wird diese dynamische Schaltfläche geklickt, so wird Vertrauen aus einem Serverzertifikat entfernt. Zurückgewiesene Zertifikate verbleiben in der Liste der vertrauenswürdigen Server und werden mit einem roten X gekennzeichnet.

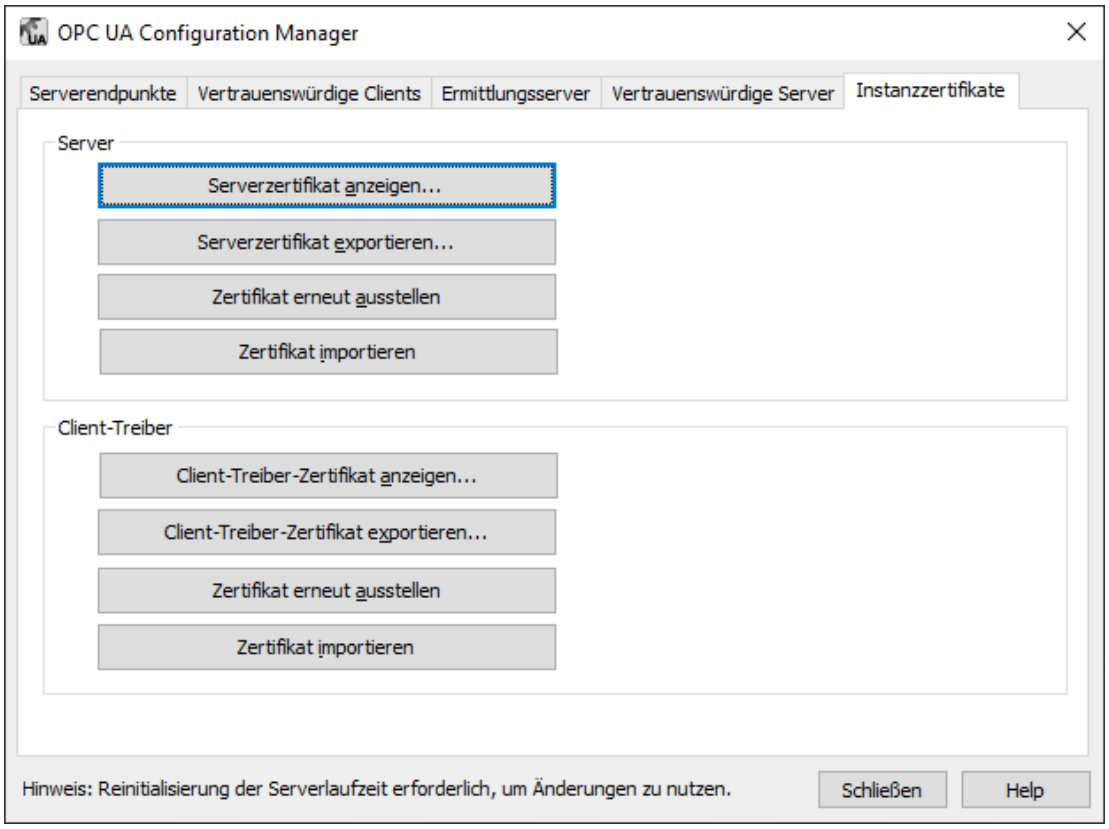
**Vertrauen**: Wird diese dynamische Schaltfläche geklickt, so wird einem Serverzertifikat vertraut.

**Zertifikat anzeigen…**: Wird diese Schaltfläche geklickt, so werden Informationen zum Serverzertifikat angezeigt.

*Anweisungen zum Austausch von Zertifikaten zwischen UA Client-Treiber und UA Server finden Sie unter* ***Manueller Austausch****.*

## Instanzzertifikate

Die selbstsignierten X.509-Instanzzertifikate wurden für den UA Server und die UA Client-Treiber geschaffen. Auf sie kann über die Registerkarte "Instanzzertifikate", wie nachfolgend gezeigt, zugegriffen werden.




### Server

**Serverzertifikat anzeigen**: Wird diese Schaltfläche geklickt, so wird das Serverzertifikat aufgerufen. Das Dialogfenster enthält neben dem Zertifikationspfad sowohl allgemeine wie auch detaillierte Zertifikatinformationen. *Weitere Informationen dazu finden Sie unter*Zertifikatanzeige.

**Serverzertifikat exportieren**: Wird diese Schaltfläche geklickt, so wird das Serverzertifikat an den gewünschten Speicherort exportiert.

**Zertifikat erneut ausstellen**: Wird diese Schaltfläche geklickt, so wird das Serverzertifikat erneut ausgestellt. Von OPC UA Configuration Manager generierte Zertifikate sind selbstsigniert, für die Signatur wurde der rsa-sha256-Algorithmus verwendet, und sie laufen nach 3 Jahren aus. Durch eine erneute Ausstellung werden vorhandene Vertrauensbeziehungen ungültig.

**Zertifikat importieren**: Wird diese Schaltfläche geklickt, so wird ein Zertifikat importiert. Importierte Serverzertifikate müssen das Format PKCS12 (eine .pfx-Erweiterung) aufweisen. Sie müssen sowohl das Instanzzertifikat als auch den privaten Schlüssel enthalten und können passwortgeschützt sein.

### Client

**Client-Treiber-Zertifikat anzeigen**: Wird diese Schaltfläche geklickt, so wird das Client-Treiber-Zertifikat aufgerufen. Das Dialogfenster enthält neben dem Zertifikationspfad sowohl allgemeine wie auch detaillierte Zertifikatinformationen. *Weitere Informationen dazu finden Sie unter*Zertifikatanzeige.

**Client-Treiber-Zertifikat exportieren**: Wird diese Schaltfläche geklickt, so wird das Client-Treiber-Zertifikat an den gewünschten Speicherort exportiert.

**Zertifikat erneut ausstellen**: Wird diese Schaltfläche geklickt, so wird das Client-Treiber-Zertifikat erneut ausgestellt. Von OPC UA Configuration Manager generierte Zertifikate sind selbstsigniert, für die Signatur wurde

der rsa-sha256-Algorithmus verwendet, und sie laufen nach 3 Jahren aus. Durch eine erneute Ausstellung werden vorhandene Vertrauensbeziehungen ungültig.

**Zertifikat importieren**: Wird diese Schaltfläche geklickt, so wird ein Zertifikat importiert. Importierte Client-Zertifikate müssen das Format PKCS12 (eine .pfx-Erweiterung) aufweisen. Sie müssen sowohl das Instanzzertifikat als auch den privaten Schlüssel enthalten und können passwortgeschützt sein.

## Selbstsignierte Standard-Zertifikate

**Dateinamen**:

- <Produktname>_ua_server.der
- <Produktname>_ua_client_driver.der

**Ablaufdatum**:

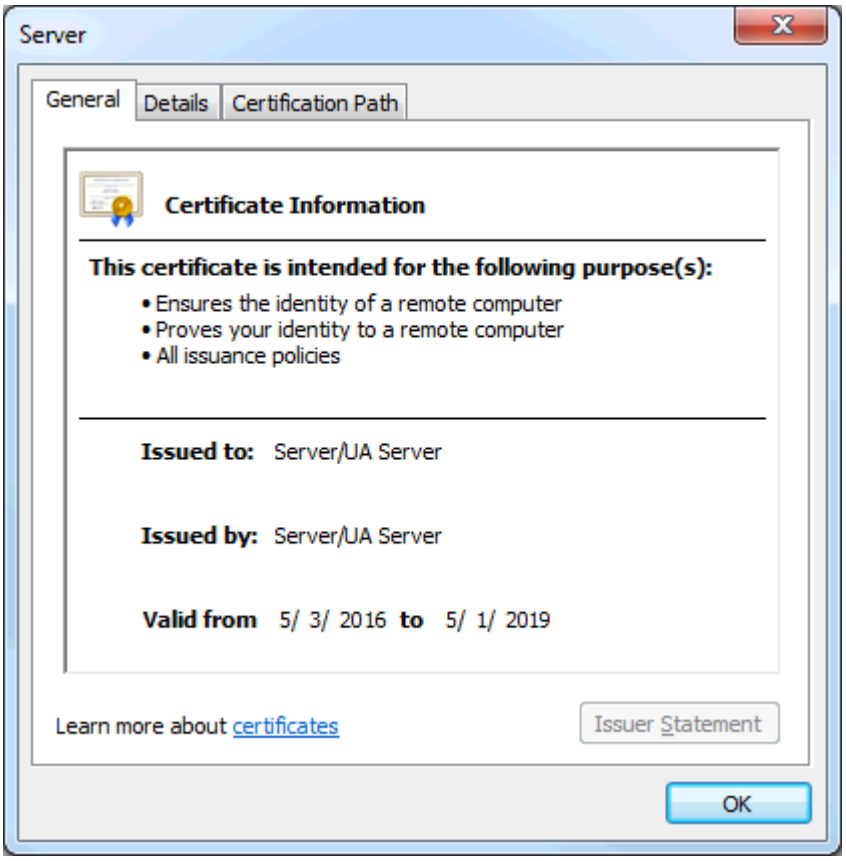
- Drei (3) Jahre nach Ausstellung.

**Signier-Algorithmus**

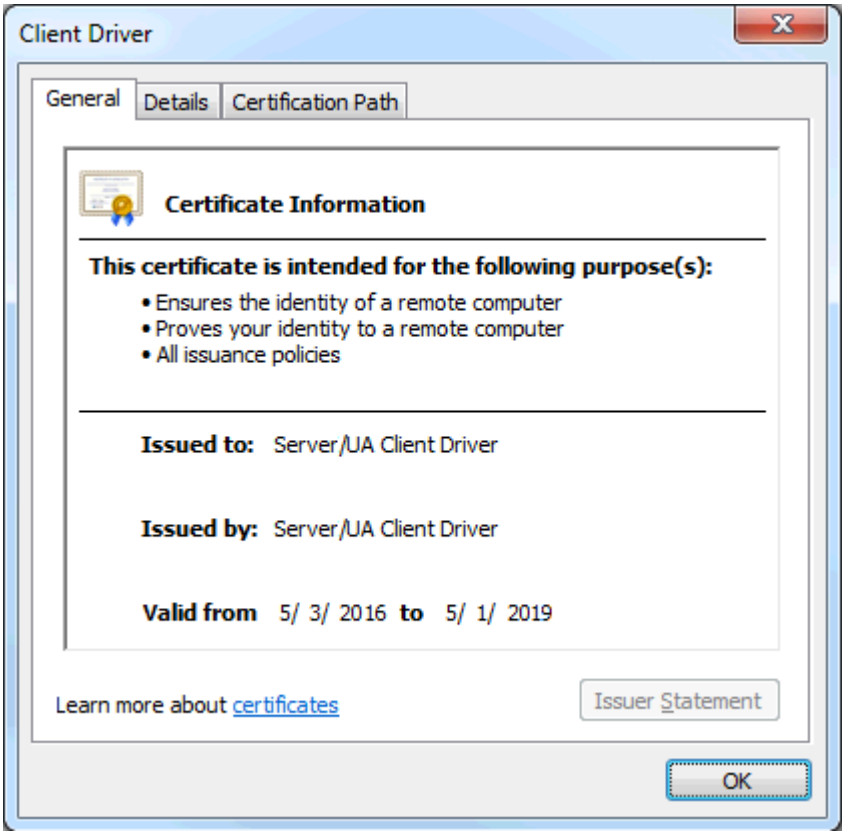
- rsa-sha256

## Zertifikatanzeige

Das Dialogfenster sollte wie folgt aussehen, wenn der Serverzertifikat anzeigt wird:




Das Dialogfenster sollte wie folgt aussehen, wenn der Client-Treiber-Zertifikat anzeigt wird:

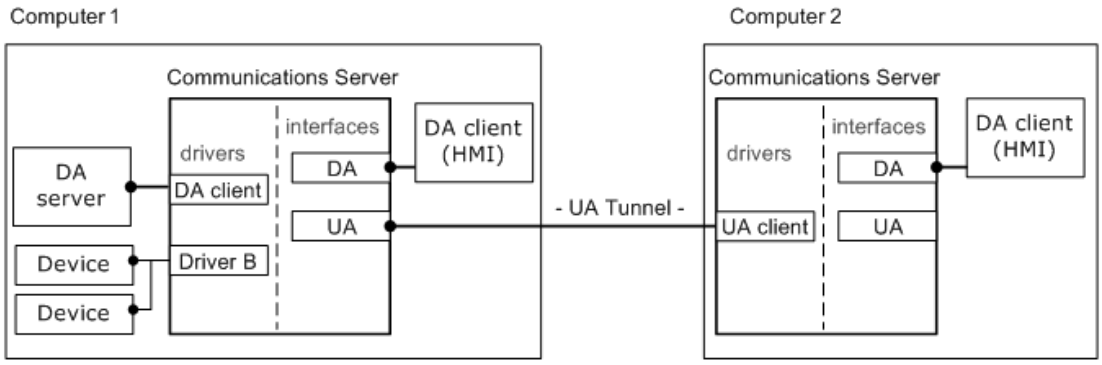

Client Driver
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• All issuance policies
Issued to: Server/UA Client Driver
Issued by: Server/UA Client Driver
Valid from 5/ 3/ 2016 to 5/ 1/ 2019
Learn more about certificates
Issuer Statement
OK

## Verbindungsbeispiele

Der OPC UA Tunnel ist kein eigentliches Produkt, sondern eine Remoteverbindungs-Lösung, die aus vorhandenen verfügbaren Komponenten erstellt wurde. Auf der Serverseite des Tunnels ist der OPC UA Server eine Benutzeroberfläche, die neben OPC DA im gesamten Kommunikationsserver-Produkt gepackt ist. Auf der Clientseite des Tunnels ist der OPC UA Client-Treiber ein Treiber-Plugin, das zusammen mit anderen Gerätekanälen hinzugefügt werden kann. OPC UA Configuration Manager ist ein Tool, das die Verwaltung von vertrauenswürdigen Zertifikaten und UA Server-Endpunkten ermöglicht. Der DA Client-Treiber ist ein zusätzliches Treiber-Plugin, welches die UA-Tunnellösung weiter verbessert. Da es sich beim Kommunikationsserver um einen "Server" handelt, bietet dieser Treiber Konnektivität zu anderen OPC DA-Servern.

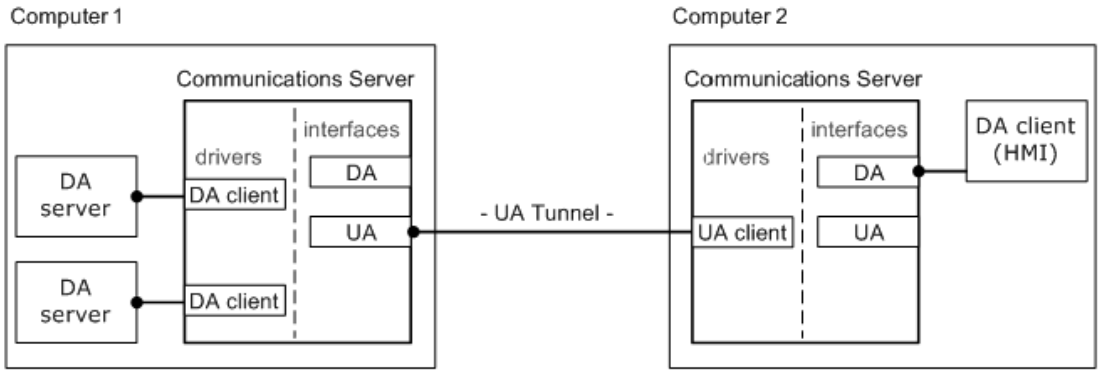
### Daten aus der Fabrik für Remote-Clients bereitstellen

Der Kommunikationsserver stellt Daten für lokale OPC DA-Clients bereit sowie für Remote-OPC DA-Clients. Die UA Tunnel-Lösung bietet die sichere Remote-Verbindung



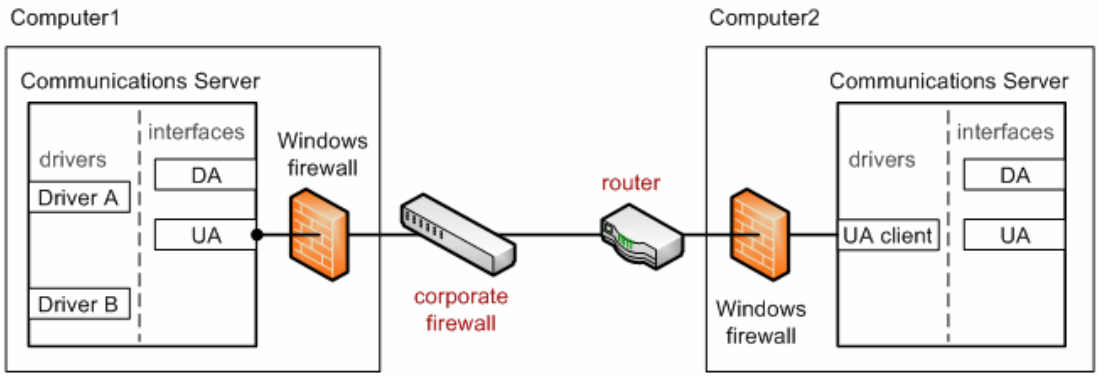

### Sichere Aggregatdaten von externen DA-Servern bereitstellen

Der Kommunikationsserver verwendet den OPC DA Client-Treiber, um eine Verbindung zu OPC DA-Servern herzustellen. Anschließend werden Aggregatdaten sicher für Remote-OPC DA-Clients bereitgestellt.




### Beispiel: Firewall und Routing-Architektur

Es ist wahrscheinlich, dass Benutzer eine Port-Ausnahme (z.B. UA-Server-Endpunkt-Port) für die Windows-Firewall auf Computer 1 erlauben müssen, zusätzlich zum Öffnen eines Ports in der Unternehmensfirewall. Für die Windows-Firewall auf Computer 2 sollten keine Änderungen erforderlich sein. Der Router auf der Client-Seite der Verbindung erfordert jedoch möglicherweise, dass ein Port geöffnet oder eine Portweiterleitungs-Option aktiviert wird.


Computer1
Communications Server
drivers
interfaces
DA
Driver A
UA
Driver B
Windows firewall
corporate firewall
router
Computer2
Communications Server
drivers
interfaces
DA
UA client
UA
Windows firewall

## Tipps zur Problembehandlung

Klicken Sie auf den Link für eine Beschreibung des Problems.

### Tipps zur Problembehandlung

Beim Versuch, Elemente in das Dialogfenster "Geräteeigenschaften" zu importieren, kann keine Verbindung zum UA Server hergestellt werden
Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen
Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird
Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden
Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort)
Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden
Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll

## Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen

### Mögliche Ursache:

1. Der im Feld "Ermittlungs-Port" aufgelistete Endpunkt-Port ist falsch.
2. Der Endpunkt ist auf dem UA Server nicht aktiviert.
3. Die UA Server-Benutzeroberfläche ist in den Projekteigenschaften deaktiviert.
4. Der UA Server und der Endpunkt sind aktiviert und richtig, Änderungen wurden jedoch nicht in der Server-Laufzeit gespeichert.

### Lösung:

1. Bestätigen Sie den im UA Server definierten Endpunkt und geben Sie den richtigen Port in das Feld "Ermittlungs-Port" ein. Aktualisieren Sie anschließend die Ansicht.
2. Starten Sie den OPC UA Configuration Manager auf dem UA Server-Computer, um sich zu vergewissern, dass der Endpunkt aktiviert ist.
3. Starten Sie die Serverkonfiguration. Prüfen Sie unter **Bearbeiten**| **Projekteigenschaften** die Eigenschaftsgruppe **OPC UA** hinsichtlich der Einstellungen für die Serverschnittstelle.
4. Stellen Sie sicher, dass **Aktivieren** auf **Ja** festgelegt ist.
5. Speichern Sie das Projekt aus der Konfiguration und klicken Sie auf **Ja**, wenn Sie dazu aufgefordert werden, die Änderungen in der Laufzeit zu speichern.

## Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird

### Mögliche Ursache:

Der Zielcomputer wurde nicht zur Netzwerk-Domäne hinzugefügt. Der Zielcomputer befindet sich möglicherweise lediglich in einer Arbeitsgruppe und nicht in einer Domäne.

### Lösung:

Bestätigen Sie die Endpunkt-URL vom UA Configuration Manager auf dem UA Servercomputer. Geben Sie anschließend die Endpunkt-URL im UA Client-Treiber-Kanal manuell ein.

## Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden

### Mögliche Ursache:

1. Die Unternehmensfirewall auf der Client-Seite der Verbindung erlaubt möglicherweise nur Verbindungen über einen einzelnen Port (wie z.B. 8080).
2. Der serverseitige Router/Switch muss so konfiguriert werden, dass eingehende Client-Anforderungen an den UA Server-Computer weitergeleitet werden.
3. Die Windows-Firewall blockiert die eingehende Anforderung vom UA-Client.

### Lösung:

1. Öffnen Sie einen Port in der Unternehmensfirewall für die UA-Tunnelverbindung. Alternativ können Sie den Endpunkt-Port auf dem UA Server zurücksetzen, so dass er dem Port entspricht, den die Unternehmensfirewall erlaubt.
2. Konfigurieren Sie Portweiterleitung im Router. Die URL des UA-Clients verwendet in diesem Fall die IP-Adresse des Routers mit der Portnummer, die für den UA Server-Endpunkt (die für die Portweiterleitung verwendete Portnummer) verwendet wird.
3. Fügen Sie eine Ausnahme für den Endpunkt-Port zur Windows-Firewall hinzu.

## Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort)

### Mögliche Ursache:

Der Client-Sitzungen-Parameter für den UA Server, **Anonyme Anmeldung zulassen** wurde auf **Nein** festgelegt.

### Lösung:

Starten Sie die Serverkonfiguration und wählen Sie ein Projekt in der Baumansicht aus. Prüfen Sie unter **Bearbeiten** | **Eigenschaften** die OPC UA Eigenschaftsgruppe hinsichtlich der Einstellungen für Client-Sitzungen und bestätig Sie, dass **Anonyme Anmeldung zulassen** auf **Ja** festgelegt ist.

### Hinweis:

Ist Authentifizierung erforderlich, greifen Sie über die Serververwaltung (in der Taskleiste) auf den Benutzermanager zu, um den Benutzernamen und das Passwort festzulegen.

## Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden

### Mögliche Ursache:

Die Standardeinstellung des Routers ist möglicherweise, nicht auf das Pingen zu reagieren.

### Lösung:

Aktivieren Sie auf der Serverseite des Routers, dass auf das Pingen reagiert wird. Deaktivieren Sie diese Einstellung, nachdem erfolgreich auf das Pingen reagiert wurde.

## Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll

### Mögliche Ursache:

OPC UA Serverdiagnose ist nicht aktiviert.

### Lösung:

Starten Sie die Serverkonfiguration und wählen Sie **Projekt** in der Baumansicht aus. Wählen Sie **Bearbeiten** | **Projekteigenschaften**. Suchen Sie auf der Registerkarte UA nach der Serverschnittstelle und bestätigen Sie, dass "Protokolldiagnose" auf "Ja" festgelegt ist.

# Ereignisprotokollmeldungen

Die folgenden Informationen betreffen Meldungen, die im Fensterbereich Ereignisprotokoll in der Hauptbenutzeroberfläche angezeigt werden. Informationen zum Filtern und Sortieren der Detailansicht Ereignisprotokoll finden Sie in der OPC-Serverhilfe. In der Serverhilfe sind viele allgemeine Meldungen enthalten, die also auch gesucht werden sollten. Im Allgemeinen werden die Art der Meldung (Information, Warnung) sowie Fehlerbehebungsinformationen bereitgestellt (sofern möglich).

## Konto '<Name>' hat keine Berechtigung zum Ausführen der Anwendung.

### Fehlertyp:
Fehler

### Mögliche Ursache:
Der derzeit angemeldete Benutzer verfügt nicht über ausreichende Berechtigungen.

### Mögliche Lösung:

1. Melden Sie sich mit einem Administrator-Konto an.
2. Wenden Sie sich an den Systemadministrator, um Berechtigungen zu verifizieren oder zu aktualisieren.
3. Verifizieren oder korrigieren Sie die Zugriffsrechte für das Anwendungsdatenverzeichnis für diese Anwendung.

### Siehe auch:
Anwendungsdaten (in der Server-Hilfe) und der Abschnitt "Benutzerberechtigungen für Anwendungsdaten" des Handbuchs <a href="https://www.kepware.com/getattachment/6882fe00-8e8a-432b-b138-594e94f8ac88/kepserverex-secure-deployment-guide.pdf">Sichere Bereitstellung von \nThingWorx Kepware Server</a>

## Das Zertifikat des UA Server wurde erneut ausgestellt. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen.

### Fehlertyp:
Sicherheit

## Das Zertifikat des UA Client Treibers wurde erneut ausgestellt. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann.

### Fehlertyp:
Sicherheit

## Das UA Client Zertifikat '<Client-Name>' wurde zurückgewiesen. Der Server kann keine Verbindungen von dem Client annehmen.

### Fehlertyp:
Sicherheit

## Das UA Client Zertifikat '<Client-Name>' wurde als vertrauenswürdig eingestuft. Der Server kann Verbindungen von dem Client annehmen.

### Fehlertyp:
Sicherheit

### Das UA Server Zertifikat '<Servername>' wurde zurückgewiesen. Der UA Client Treiber kann keine Verbindung zum Server herstellen.

**Fehlertyp:**
Sicherheit

### Das UA Server Zertifikat '<Servername>' wurde als vertrauenswürdig eingestuft. Der UA Client Treiber kann eine Verbindung zum Server herstellen.

**Fehlertyp:**
Sicherheit

### Das UA Server Zertifikat '<Servername>' wurde zur Liste der vertrauenswürdigen Server hinzugefügt. Der UA Client Treiber kann jetzt eine Verbindung zum Server herstellen.

**Fehlertyp:**
Sicherheit

### Das UA Client Zertifikat '<Client-Name>' wurde zur Liste der vertrauenswürdigen Clients hinzugefügt. Der UA Server kann jetzt Verbindungen vom Client annehmen.

**Fehlertyp:**
Sicherheit

### Das UA Client Zertifikat '<Client-Name>' wurde aus der Liste der vertrauenswürdigen Clients entfernt. Der UA Server kann keine Verbindungen vom Client annehmen.

**Fehlertyp:**
Sicherheit

### Das UA Server Zertifikat '<Servername>' wurde aus der Liste der vertrauenswürdigen Server entfernt. Der UA Client Treiber kann keine Verbindung zum Server herstellen.

**Fehlertyp:**
Sicherheit

### Der Endpunkt '<URL>' wurde zum UA Server hinzugefügt.

**Fehlertyp:**
Sicherheit

### Der Endpunkt '<URL>' wurde vom UA Server entfernt.

**Fehlertyp:**
Sicherheit

### Der UA Discovery Server '<Servername>' wurde hinzugefügt. Die UA Server Endpunkte können jetzt mit diesem UA Discovery Server registriert werden.

**Fehlertyp:**
Sicherheit

### Der UA Discovery Server '<Servername>' wurde entfernt. Die UA Server Endpunkte können nicht länger mit diesem UA Discovery Server registriert werden.

**Fehlertyp:**
Sicherheit

### Der Endpunkt '<URL>' wurde deaktiviert.

**Fehlertyp:**
Sicherheit

### Das Zertifikat des UA Client Treibers wurde importiert. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann.

**Fehlertyp:**
Sicherheit

### Das Zertifikat des UA Server wurde importiert. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen.

**Fehlertyp:**
Sicherheit

### Der Endpunkt '<URL>' wurde aktiviert.

**Fehlertyp:**
Sicherheit

### Vertrauenswürdigen Client hinzufügen

Das UA Client-Zertifikat '<Zertifikatname>' wurde zu den vertrauenswürdigen Clients hinzugefügt. Der UA Server akzeptiert jetzt Verbindungen vom Client.

### Vertrauenswürdigen Client entfernen

Das UA Client-Zertifikat '<Zertifikatname>' wurde aus den vertrauenswürdigen Clients entfernt. Der UA Server akzeptiert keine Verbindungen von diesem Client.

### Vertrauenswürdigen Client ablehnen

Das UA Client-Zertifikat '<Zertifikatname>' wurde abgelehnt. Der Server akzeptiert keine Verbindungen von diesem Client.

### Vertrauenswürdigem Client vertrauen

Dem UA Client-Zertifikat '<Zertifikatname>' wurde vertraut. Der Server akzeptiert keine Verbindungen vom Client.

### Vertrauenswürdigen Server hinzufügen

Das UA Server-Zertifikat '<Zertifikatname>' wurde zu den vertrauenswürdigen Servern hinzugefügt. Der UA Client-Treiber kann jetzt eine Verbindung zum Server herstellen.

### Vertrauenswürdigen Server entfernen

Das UA Server-Zertifikat '<Zertifikatname>' wurde aus den vertrauenswürdigen Servern entfernt. Der UA Client-Treiber kann keine Verbindung zum Server herstellen.

## Vertrauenswürdigen Server ablehnen

Das UA Server-Zertifikat '<Zertifikatname>' wurde abgelehnt. Der UA Client-Treiber kann keine Verbindung zum Server herstellen.

## Vertrauenswürdigem Server vertrauen

Dem UA Server-Zertifikat '<Zertifikatname>' wurde vertraut. Der UA Client-Treiber kann keine Verbindung zum Server herstellen.

## Endpunkt hinzufügen

Der Endpunkt '<Endpunktdefinition>' wurde zum UA Server hinzugefügt.

## Endpunkt aktivieren

Der Endpunkt '<Endpunktdefinition>' wurde aktiviert.

## Endpunkt deaktivieren

Der Endpunkt '<Endpunktdefinition>' wurde deaktiviert.

## Endpunkt entfernen

Der Endpunkt '<Endpunktdefinition>' wurde aus dem UA Server entfernt.

## Ermittlungsserver hinzufügen

Der Ermittlungsserver '<Zertifikatname>' wurde hinzugefügt. Die UA Server-Endpunkte registrieren sich jetzt mit dem Ermittlungsserver.

## Ermittlungsserver entfernen

Der Ermittlungsserver '<Zertifikatname>' wurde entfernt. Die UA Server-Endpunkte registrieren sich nicht länger mit diesem Ermittlungsserver.

## Client-Zertifikat erneut ausstellen

Das UA Client-Treiber-Zertifikat wurde erneut ausgestellt. UA Server müssen dem neuen Zertifikat vertrauen, damit der Client-Treiber eine Verbindung herstellen kann.

## Serverzertifikat erneut ausstellen

Das UA Server-Zertifikat wurde erneut ausgestellt. Die UA Clients müssen diesem neuen Zertifikat vertrauen, um eine Verbindung herzustellen.

# Index

## C

Client-Zertifikat erneut ausstellen 21

## D

Das UA Client Zertifikat '<Client-Name>' wurde als vertrauenswürdig eingestuft. Der Server kann Verbindungen von dem Client annehmen. 18

Das UA Client Zertifikat '<Client-Name>' wurde aus der Liste der vertrauenswürdigen Clients entfernt. Der UA Server kann keine Verbindungen vom Client annehmen. 19

Das UA Client Zertifikat '<Client-Name>' wurde zur Liste der vertrauenswürdigen Clients hinzugefügt. Der UA Server kann jetzt Verbindungen vom Client annehmen. 19

Das UA Client Zertifikat '<Client-Name>' wurde zurückgewiesen. Der Server kann keine Verbindungen von dem Client annehmen. 18

Das UA Server Zertifikat '<Servername>' wurde als vertrauenswürdig eingestuft. Der UA Client Treiber kann eine Verbindung zum Server herstellen. 19

Das UA Server Zertifikat '<Servername>' wurde aus der Liste der vertrauenswürdigen Server entfernt. Der UA Client Treiber kann keine Verbindung zum Server herstellen. 19

Das UA Server Zertifikat '<Servername>' wurde zur Liste der vertrauenswürdigen Server hinzugefügt. Der UA Client Treiber kann jetzt eine Verbindung zum Server herstellen. 19

Das UA Server Zertifikat '<Servername>' wurde zurückgewiesen. Der UA Client Treiber kann keine Verbindung zum Server herstellen. 19

Das Zertifikat des UA Client Treibers wurde erneut ausgestellt. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. 18

Das Zertifikat des UA Client Treibers wurde importiert. UA Server müssen das neue Zertifikat als vertrauenswürdig einstufen, damit der Client-Treiber eine Verbindung herstellen kann. 20

Das Zertifikat des UA Server wurde erneut ausgestellt. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. 18

Das Zertifikat des UA Server wurde importiert. UA Clients müssen das neue Zertifikat als vertrauenswürdig einstufen, um eine Verbindung herzustellen. 20

Der Endpunkt '<URL>' wurde aktiviert. 20

Der Endpunkt '<URL>' wurde deaktiviert. 20

Der Endpunkt '<URL>' wurde vom UA Server entfernt. 19

Der Endpunkt '<URL>' wurde zum UA Server hinzugefügt. 19

Der UA Discovery Server '<Servername>' wurde entfernt. Die UA Server Endpunkte können nicht länger mit diesem UA Discovery Server registriert werden. 20

Der UA Discovery Server '<Servername>' wurde hinzugefügt. Die UA Server Endpunkte können jetzt mit diesem UA Discovery Server registriert werden. 19

Der UA Server wird nicht erkannt, wenn versucht wird, vom UA Client aus zu durchsuchen 15

Der Versuch, eine Verbindung zum UA Server herzustellen, erfordert Authentifizierung (Benutzername und Passwort) 16

## E

Endpunkt aktivieren 21

Endpunkt deaktivieren 21
Endpunkt entfernen 21
Endpunkt hinzufügen 21
Endpunktdefinition 5
Ereignisprotokollmeldungen 18
Ermittlungsserver 7
Ermittlungsserver entfernen 21
Ermittlungsserver hinzufügen 21
Exportieren 7-8
Externe DA Server 13

## F

Firewall 13

## I

Importieren 7-8
Inhalt der Hilfe 4
Instanzzertifikate 10

## K

Keine OPC UA spezifischen Fehlermeldungen im Ereignisprotokoll 16
Konto '<Name>' hat keine Berechtigung zum Ausführen der Anwendung. 18

## N

Netzwerkadapter 6

## O

OPC Data Access (DA) 4
OPC Foundation 4
OPC UA Configuration Manager 5
OPC Unified Architecture (UA) 4

## P

Port-Nummer 6

## R

Registrierungsintervall 8
Remote-Clients 13
Router, der Portweiterleitung zum Senden von Anforderungen an den Server verwendet, kann nicht gepingt werden 16

## S

Serverendpunkte 5
Serverzertifikat erneut ausstellen 21
Sicherheitsrichtlinien 6
Standard-Zertifikat 11

## T

Tipps zur Problembehandlung 15

## U

Über die richtige Endpunkt-URL kann keine Verbindung zum UA Server hergestellt werden 16
Übersicht 4

## V

Verbindungsbeispiele 13
Vertrauen 7
Vertrauenswürdige Clients 7
Vertrauenswürdige Server 8
Vertrauenswürdigem Client vertrauen 20
Vertrauenswürdigem Server vertrauen 21
Vertrauenswürdigen Client ablehnen 20
Vertrauenswürdigen Client entfernen 20
Vertrauenswürdigen Client hinzufügen 20
Vertrauenswürdigen Server ablehnen 21
Vertrauenswürdigen Server entfernen 20
Vertrauenswürdigen Server hinzufügen 20

## Z

Zertifikat 9
Zertifikat anzeigen 7

Zertifikat erneut ausstellen 10

Zertifikat importieren 10-11

Zertifikatanzeige 11

Zielcomputer, auf dem der UA Server ausgeführt wird, wird nicht im Netzwerk angezeigt, wenn vom UA Client aus durchsucht wird 15